Crime Mapping and Data Confidentiality Roundtable July 8-9, 1999

Sponsored by: National Institute of Justice, Crime Mapping Research Center

Accountability for Inappropriate Use of Crime Maps And the Sharing of Inaccurate Data

by
James W. Meeker, J.D, Ph.D.
University of California, Irvine

I have been asked to comment on *when information passes from one agency to another, who is liable or accountable for the inappropriate use of crime maps or the sharing of inaccurate, geocoded data and what kind of disclaimers should be made*. In my opinion, this is a fairly broad and potentially complex topic not subject to a one or two page summary. Given I have had only a short time to research some narrow issues on this topic please treat this document as a draft and a tentative statement of ideas that are still developing.

In order to narrow the problem, several simplifying assumptions are needed. First, I am assuming that the maps in question will be the type that law enforcement uses in showing the general spatial distribution of crime such as pin maps or hot spots (various clustering techniques for spatial point pattern analysis). Second, I will be addressing the legal nature of such data, as I understand it under California State law. While California's Public Records Act (CPRA) Government Code §§ 6250-6270, is patterned after the federal Freedom of Information Act there are some differences. It is very likely most legal actions against law enforcement agencies on this issue would rely on state law. In addition, the recent decisions of the Supreme Court concerning state's rights and immunity from federal statutory liability, potentially could influence the application of federal law against state and local law enforcement agencies, who are most likely to publicize the type of mapping information with which we are concerned.

The first issue to address is, are such data public records? Assuming most mapping applications will rely on police report data, the public status of these records is important. Under CPRA, actual police reports and investigative files are not public, however much of the information they contain are. Relevant for mapping purposes §6254 (f) requires that state and local law enforcement agencies shall make public:
Subsection (1)
the full name and occupation of every individual arrested by the agency,
the individual's physical description,

time and date of arrest and booking,
location of arrest, factual circumstances surrounding the arrest,
the amount of bail set, the time and manner of release or the location where the individual is currently being held,
all charges the individual is being held upon, including any outstanding warrants from other jurisdictions and parole or probation holds.
Subsection (2)
time, substance, and location of all complaints or requests for assistance received by the agency and the time and nature of the response there to, including, to the extent the information regarding crimes alleged or committed or any other incident investigated is recorded, the time, date, and location of occurrence,
the time and date of the report,
the name and age of the victim
the factual circumstances surrounding the crime or incident,
general description of any injuries, property, or weapons involved.

Subsection (2) comes with several limitations on releasing the information covered. Address and phone numbers of potential witnesses or victims can not be released to potential defendants. In addition, victims or their guardians, of certain enumerated sex crimes, adoption for fee crimes, child abuse crimes, spousal abuse crimes and certain harassment crimes, may request that their name be withheld. This is an affirmative right that has to be requested by the victim.

Subsections (1) and (2) are fairly broad, covering most mapping applications of arrested individuals, crimes known to police, call for service and location of victims. Mapping the spatial distribution of suspects falls more in the area of investigative data, which has some protection from disclosure under CPRA.

Law enforcement agencies cannot refuse access to public data. Since the public has access to the data, there should be no liability attached to publishing the data, either in tabular form, or by presenting it in spatial form such as mapping. Some have expressed concern about whether a law enforcement agency would be responsible for the irresponsible or illegal use of published mapped data such as red lining by banks for high crime neighborhoods. The courts have opposed the idea of selective disclosure of public records, even if done so to protect the public. In Black Panther Party v. Kehoe 42 Cal.App3d 649, 117 Cal. Rptr. 106 (1974) the California Court of Appeal held: The term public inspection necessarily implies general, nonselective disclosure. It implies that public officials may not favor one citizen with disclosures denied to another. When a record loses its exempt status and becomes available for public inspection, section 6253, subdivision (a), endows every citizen with a right to inspect it. 117 Cal. Rptr. 106, 113.

The California Supreme Court went even further in a case involving nonexempt information contained in intelligence files involving organized crime, American Civil Liberties Union v. Deukmejian 32 Cal. 3d 440, 186 Cal. Rptr. 235, 651 P. 2d 822

(1982).
Our interpretation of subdivision (f) also derives from the fact that the Act imposes no limits upon who may seek information or what he may do with it.... In other cases, however, information may be sought for less noble purposes. Persons connected with organized crime may seek to discover what the police know, or do not know, about organized criminal activities (cite omitted); persons seeking to damage the reputation of another may try to discover if he is listed as an organized crime figure or as an associate of such a figure; other persons may simply try to put the state to the burden and expense of segregating exempt and nonexempt information and making the latter available to the public. In short, once information is held subject to disclosure under the Act, the courts can exercise no restraint on the use to which it may be put. 651 P. 2d 822, 828.

Since the law places no limits on what may be done with public information, it follows that law enforcement agencies are not responsible for misuse of public information it is required by law to release. While I could find no case law directly on point, it is doubtful that principle would be limited by the form by which the data is made public (for example, simple listing of incident addresses versus mapping).

There is some concern that by presenting public information through maps it could lead to liability because it could disclose information that is otherwise non-public. For example, maps of the location for certain sex and domestic violence crimes could unintentionally reveal the address and correspondingly the identity of protected victims. Although not involving the mapping context, this issue was confronted in Baugh v. CBS, Inc. 828 F.Supp 745 (N.D.Cal. 1993). This case involved a television news magazine filming crime victims that was sued by a victim of domestic violence. The claim was that the victim's identity was illegally disclosed. The court noted that CPRA allows for the disclosure of the location of the crime, even though in this case, it effectively disclosed the victim's address. The court also noted that the name of the victim is withheld only if the victim makes a formal request, which was not done. Here the court upheld the information disclosure as legal(see 828 F.Supp 745, 755 ftnt. 4). It would appear that crime location data, even that which leads to identification, would still be deemed public.

Maps that are inaccurate may be incorrect based on different sources of error. There are at least three, if not more, sources of error. First, there can be data error, incorrect criminal incident data such as incorrect address, crime, and factors associated with the crime data. Second, there can be incorrect base map data, for example where streets and boundaries are incorrect. Finally there can be misinterpretation of maps. In this case the inaccuracies are not so much error but in false implications a map may give, especially when viewed by untrained observers.

As for data that is erroneous, as long as it is not intentionally released knowing it is in error, or negligence is involved, I don't think there would be a serious liability issue of releasing public information that contains some error. The states have generally been

unsuccessful in suing the US Census Bureau to correct known errors involving under counting of poor and minority communities. In fact, much of the case law surrounding CPRA and FOIA contains language arguing that one of the main functions of such legislation is to give the public access to government data so that errors can be corrected.

Since base maps and their underlying information are generally not created by law enforcement agencies, I think liability for errors here can be limited by citing the source of the underlying information used. If an agency consistently uses such data it knows is in serious error, this negligence could give rise to liability issues.
Errors of misinterpretation are more elusive and difficult to control. On the one hand, this type of problem is less likely to give rise to legal liability, especially when dealing with public records. On the other, it is this kind of problem that gives pause to many law enforcement agencies in making maps publicly available. My experience with the Orange County Gang Incident Tracking System (GITS), has been that it is this fear of misinterpretation that has produced the most resistance to making public maps of gang crime data. It is the fear that misinterpretation of the data will give rise to negative community impact (such as reduced business and real estate prices) which will create negative political pressure on law enforcement.

Experience with Orange County's GITS has identified two types of misinterpretation errors. The first involves the limits of the crime data and the second involves the failure to control for relevant factors. Misinterpretation involving the limits of the data is best explained by way of example. Assume a large park, several blocks square, which is bounded by different types of zones. On one side is a commercial strip mall shopping area, another side is zoned single family resident, another is high density apartments and the last side is light industrial. Assume that gang crime is randomly distributed across the zones, but is highly concentrated in the park. The park, however, has a single address, which is what is recorded in the police reports, even though incidents take place throughout the park. A spatial point pattern analysis map is done using some of the various nearest neighborhood type techniques to examine hot spots. The hot spot can be very misleading and will unduly paint the zone that is opposite the park address as being more than randomly gang active. The problem occurs because of the relative precision of the crime data varies by area. For the zones the addresses are much more precise than the park, yet it is the park that has the highest activity. There are ways to deal with this, like geocoding the address of the park to the central point of its area, instead of using its address. The point is that mere address data may not be precise enough to represent the reality a map may be projecting.

The second type of misinterpretation problem involves failure to control for relevant factors. By way of illustration, assume we are again mapping gang hot spots. In this case we do not take into account relative density of population and potential victims. So areas like shopping centers, beaches, and amusement parks may be relatively hot because of the higher levels of human concentrations, but the actual rate of crime per population is low. This can't be controlled for with easily available census population

data, because such data don't usually reflect temporary densities (such as day use of beaches and parks). The irony is that the map will show these areas as hot spots, while the actual probably of victimization may be much lower than other so called safer areas. Such misinterpretations of maps can have major political and commercial implications.

I have observed two strategies by law enforcement to the misinterpretation problem, what I call the head in the sand policy versus the heads up policy. One response is to not to create maps and only release data when compelled to do so by law. I think this is ineffective and in the long run will increase the misinterpretation problem. As explained above, most of this information is public record. While law enforcement is not required to make the data available in map form, the advent of easy to use mapping programs will make it increasingly easier for the public and media to create their own maps. This will radically increase the likelihood of misinterpretation problems and in the long will make community relations with law enforcement more difficult. The heads up policy is to proactively release maps and data to the public but to so in a way that will minimize misinterpretation. This will require a closer working relationship between law enforcement, local government, business, and the community to ensure the correct interpretation is given. As one police chief has said, "I know they can get the information any way. It is better for me to preempt demands by releasing the data in a manner I can influence rather than create mistrust by requiring litigation, which in the end, will allow the public to analyze the data without my input."

I think this is where NIJ's CMRC can be of great assistance to law enforcement. They can take the lead and explore standard ways of presenting such mapping data that will minimize misinterpretation and make this available to law enforcement. They can also help draft standards and procedures for making such mapping data available to the public. It would be far better for professionals who are aware of the limitations of such data to create professional standards for the courts to rely upon, rather than to have such standards created in the course of litigation.